BY- Dhananjay Trivedi



**CLOUD COMPUTING WITH AWS SERVICESPROJECT**

**Integrate Grafana with Linux Server for high cpu utilization and create a graph in Grafana.**



### Table of Contents

|  |  |
| --- | --- |
| 1. Introduction | 2 |
| 1. Architecture Overview | 2 |
| 1. Problem Statement  * Detect performance bottlenecks. * Trigger alerts for high CPU consumption. * Understand trends over time. * **Technology Used** | 3  3  3  3  3 |
| 1. Implementation  * Creating EC2 Instance * Installing transport-https software * Installing Grafana | 4  5  8  10 |
| Testing & Access the Grafana web interface | 12 |

### Introduction

Grafana is a feature-rich, open-source solution designed for monitoring and data analysis, especially effective for presenting chronological datasets. Within a Linux-based server infrastructure, tracking CPU performance plays a vital role in ensuring optimal system efficiency and uptime. When connected with Prometheus and Node Exporter, Grafana enables the acquisition and visualization of live CPU statistics through dynamic and personalized dashboards, aligned with specific observability goals.

**2.Architecture Overview**

# 

### Problem Statement

System administrators need to monitor CPU usage across Linux servers to:

1. **Detect Performance Bottlenecks**

* Identify spikes in CPU usage on EC2 instances or containers (e.g., in EKS).
* Diagnose performance degradation related to compute limitations.

1. **Trigger Alerts for High CPU Consumption**

* Automatically notify administrators when CPU usage crosses defined thresholds (e.g., >80% over 5 minutes).
* Enable proactive response to prevent service disruption.

1. **Understand Trends Over Time**

* Analyze historical CPU usage to plan scaling strategies.
* Identify patterns in workload behavior for capacity planning.
* **Technology Used**
* **Amazon Web Service**

1. **Implementation**

Sign in to AWS Management Console

1.Click on the Open Console button, and you will get redirected to AWS Console in a new browser tab.

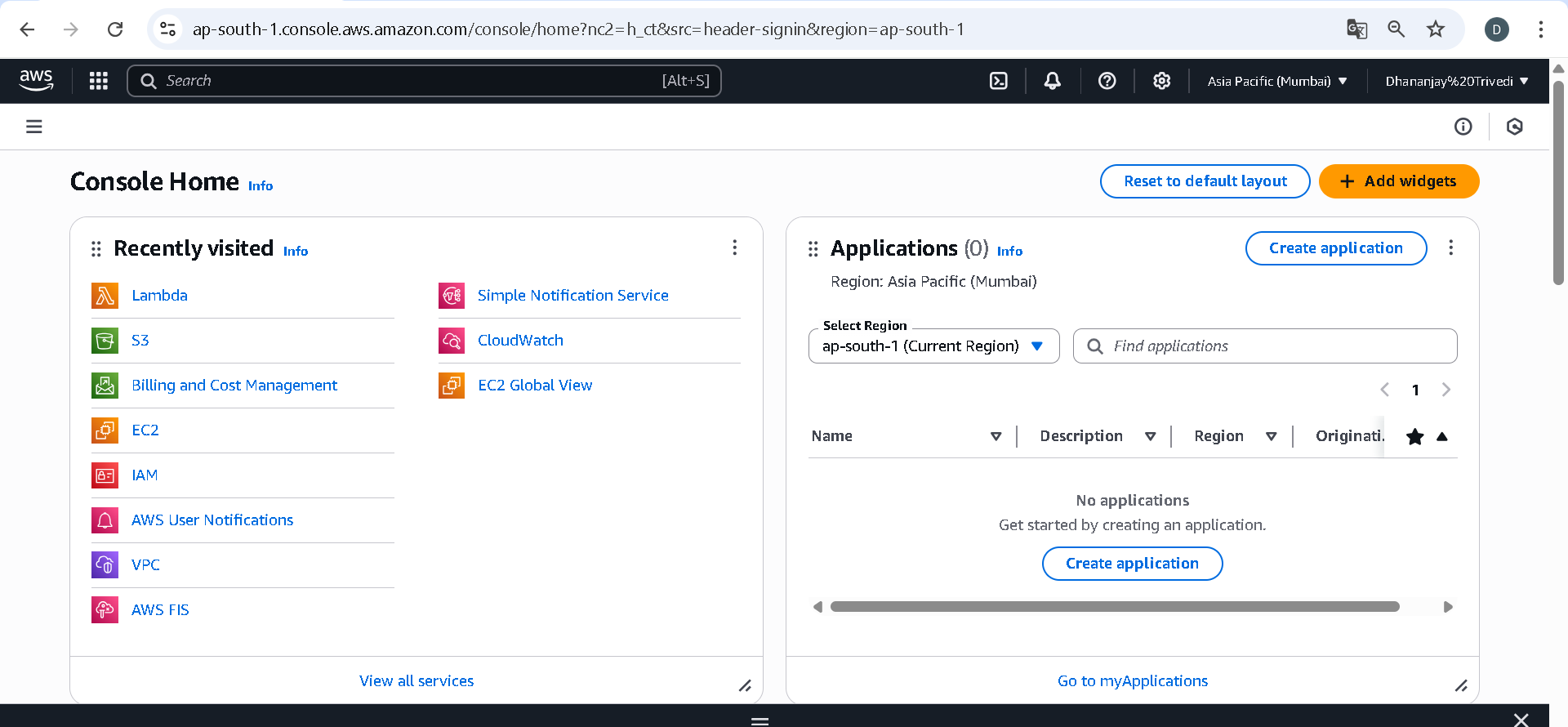
•On the AWS sign-in page, Leave the Account ID as default. Never edit/remove the 12-digit Account ID present in the AWS Console. otherwise, you cannot proceed with the lab.

•Now copy your User Name and Password in the Lab Console to the IAM

Username and Password in AWS Console and click on the Sign in button.

2.Once Signed in to the AWS Management Console, Make the default AWS Region as US East (N.

3. Asia Pacific ap-south-1

* **Creating EC2 Instance**

# For creating an EC2 instance follow the following steps as shown in snapshots.

# 

# Provide the EC2 name of your choise and select”Ubuntu”as an OS Image.

# 

# Create a new key pair. in ppk name bt your choice

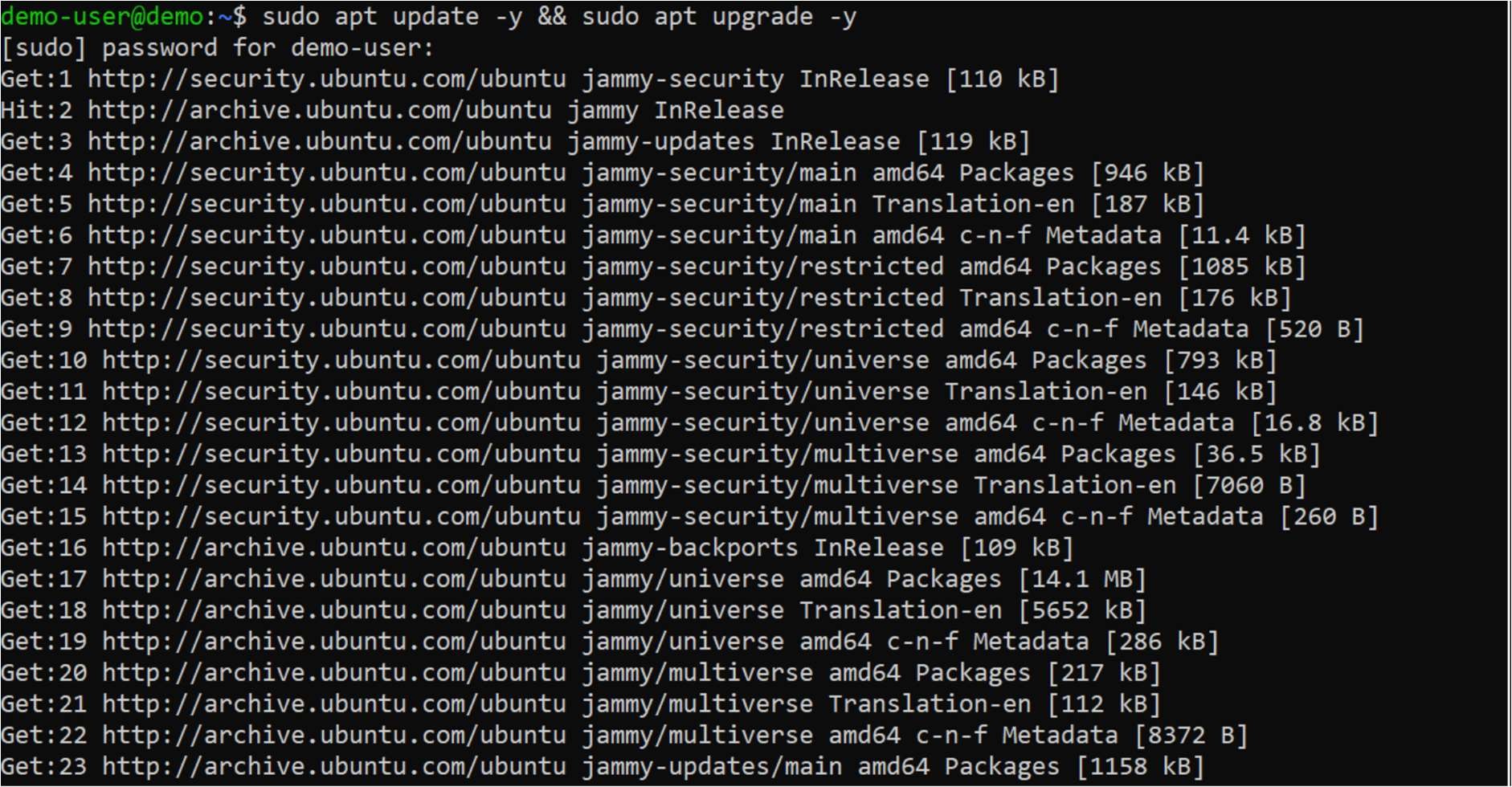
# Scroll down and click on “LAUNCH INSTANCE “.

# Then open your instancend connect that instance by putty or on web browser.

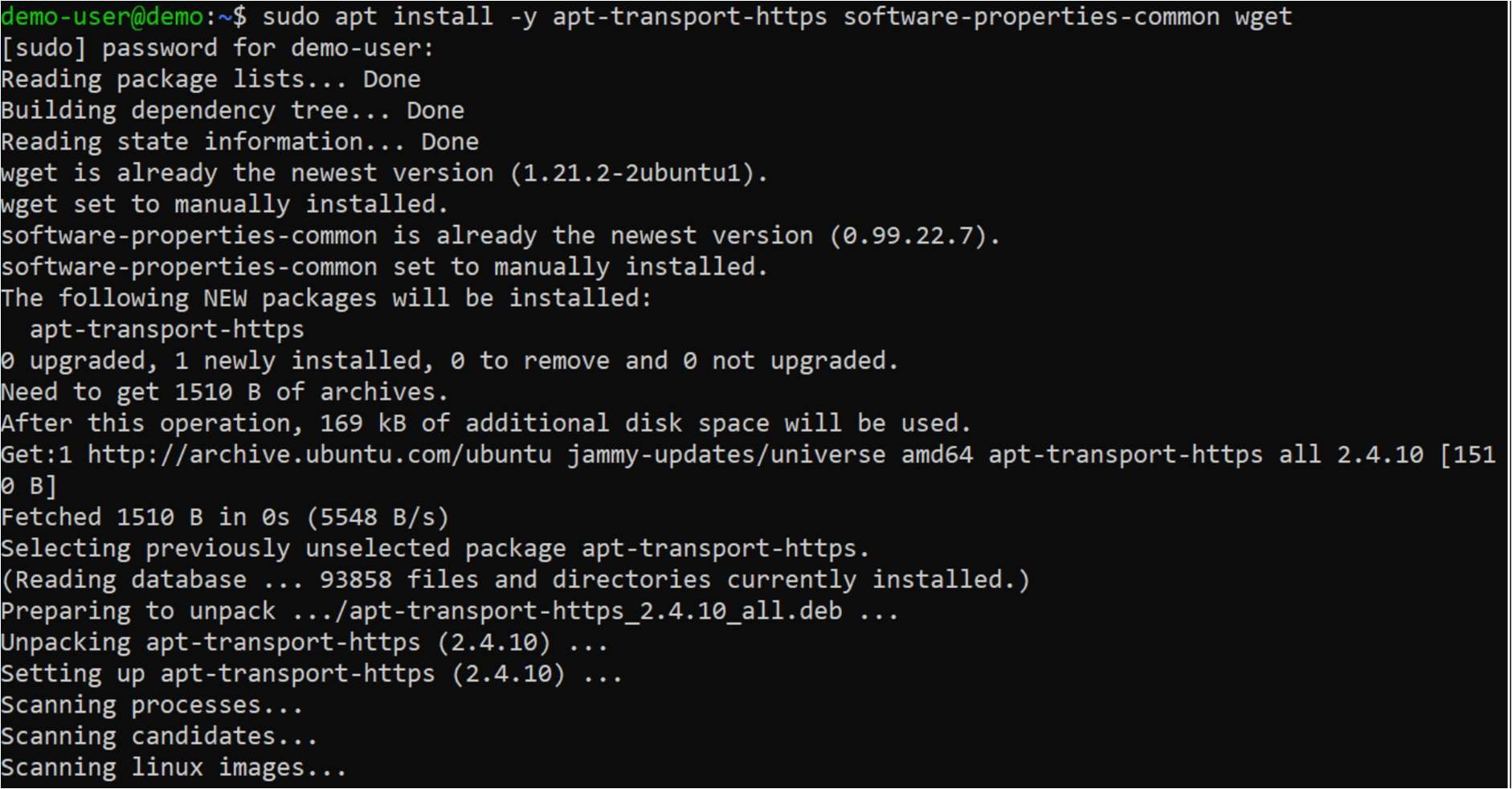
# After connecting the instance follow the given command or read Grafana documentation for help.

# **Update and upgrade**

sudo apt update -y && sudo apt upgrade –y



* + **Step 1 - Installing Transport-https Software**
* Next, run the following command to install the packages needed for the installation:

sudo apt install -y apt-transport-https software-properties-common wget

# **Step 2 - Add the Grafana GPG key**

sudo mkdir -p /etc/apt/keyrings/

wget -q -O - https://apt.grafana.com/gpg.key | gpg --dearmor | sudo tee

/etc/apt/keyrings/grafana.gpg > /dev/null

* The first command creates a directory where the key will be stored. The second command will download, convert, and store the key in the specified location for secure APT package management.



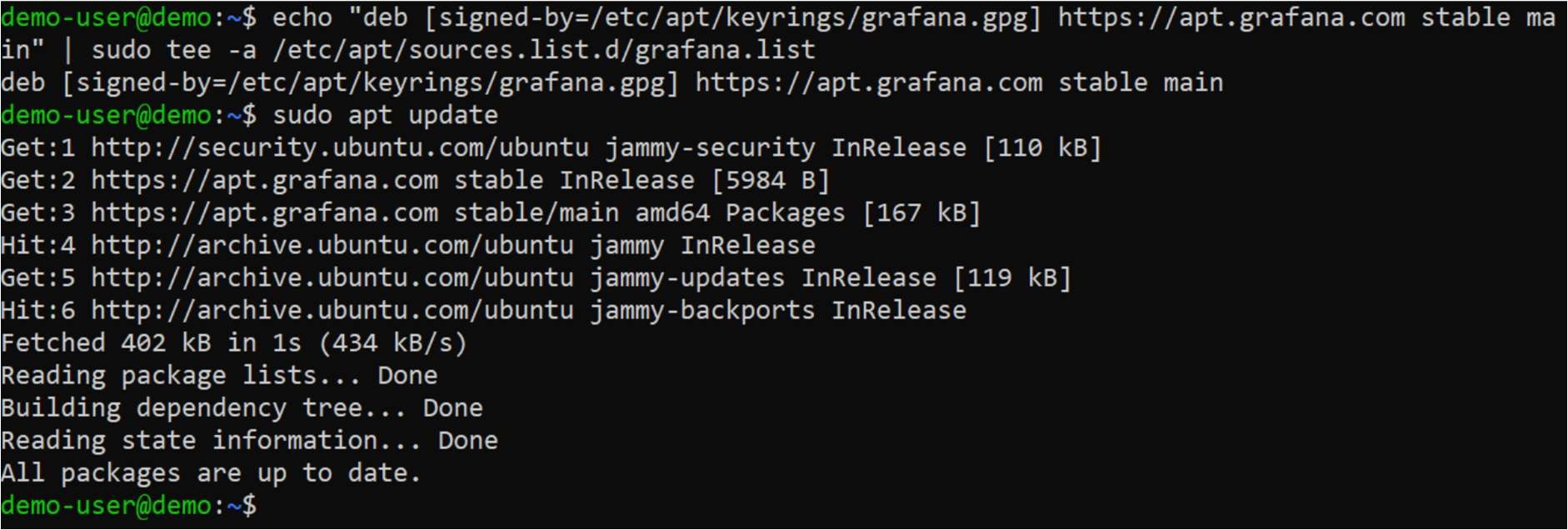
# **Step 3 - Add Grafana APT repository**

echo "deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com stable main" | sudo tee -a

/etc/apt/sources.list.d/grafana.list

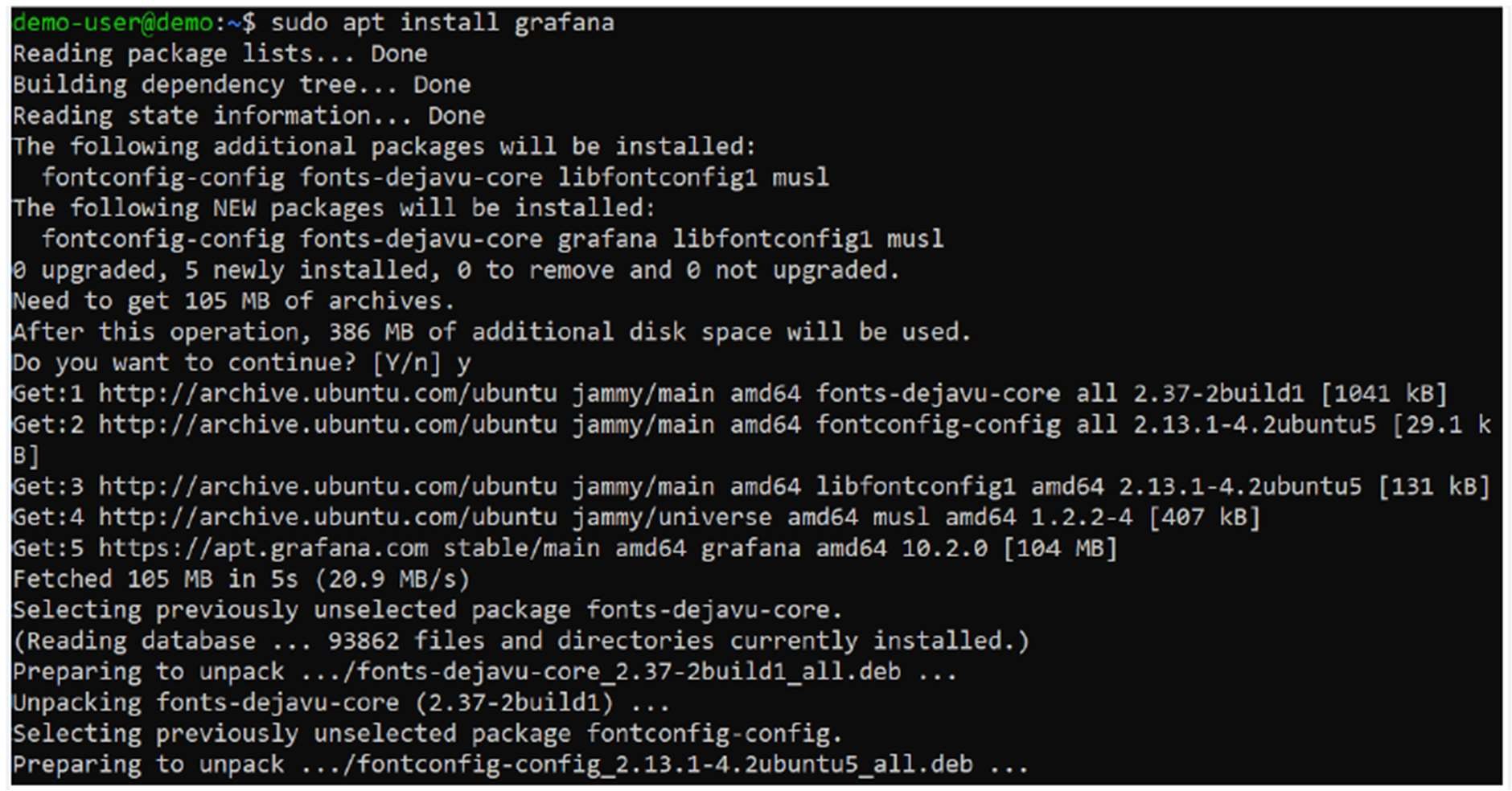
After adding the repository to your system, update the package index to include information from the newly added repository using:

sudo apt update



# **Step 4 - Install Grafana**

sudo apt install Grafana

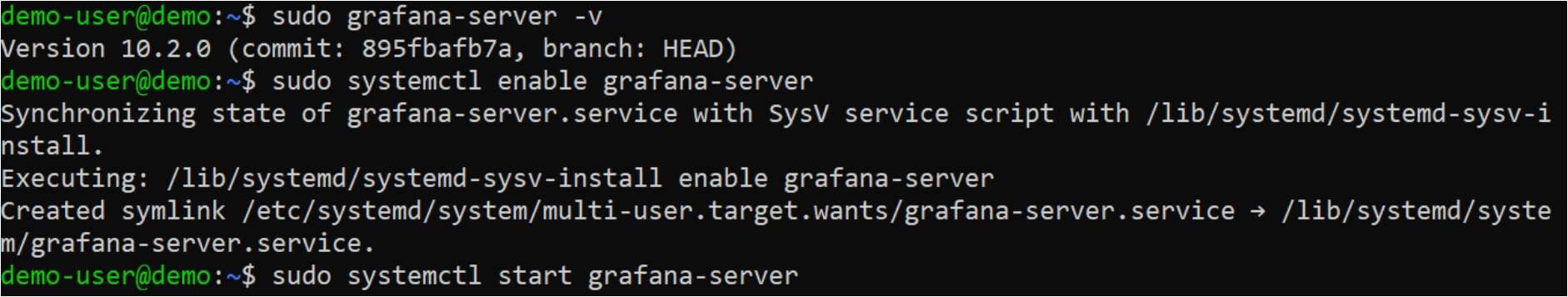


# **Step 5 - Start the Grafana service**

sudo grafana-server –v

* Next, start the Grafana service and enable it to start automatically at system reboot using the following commands:

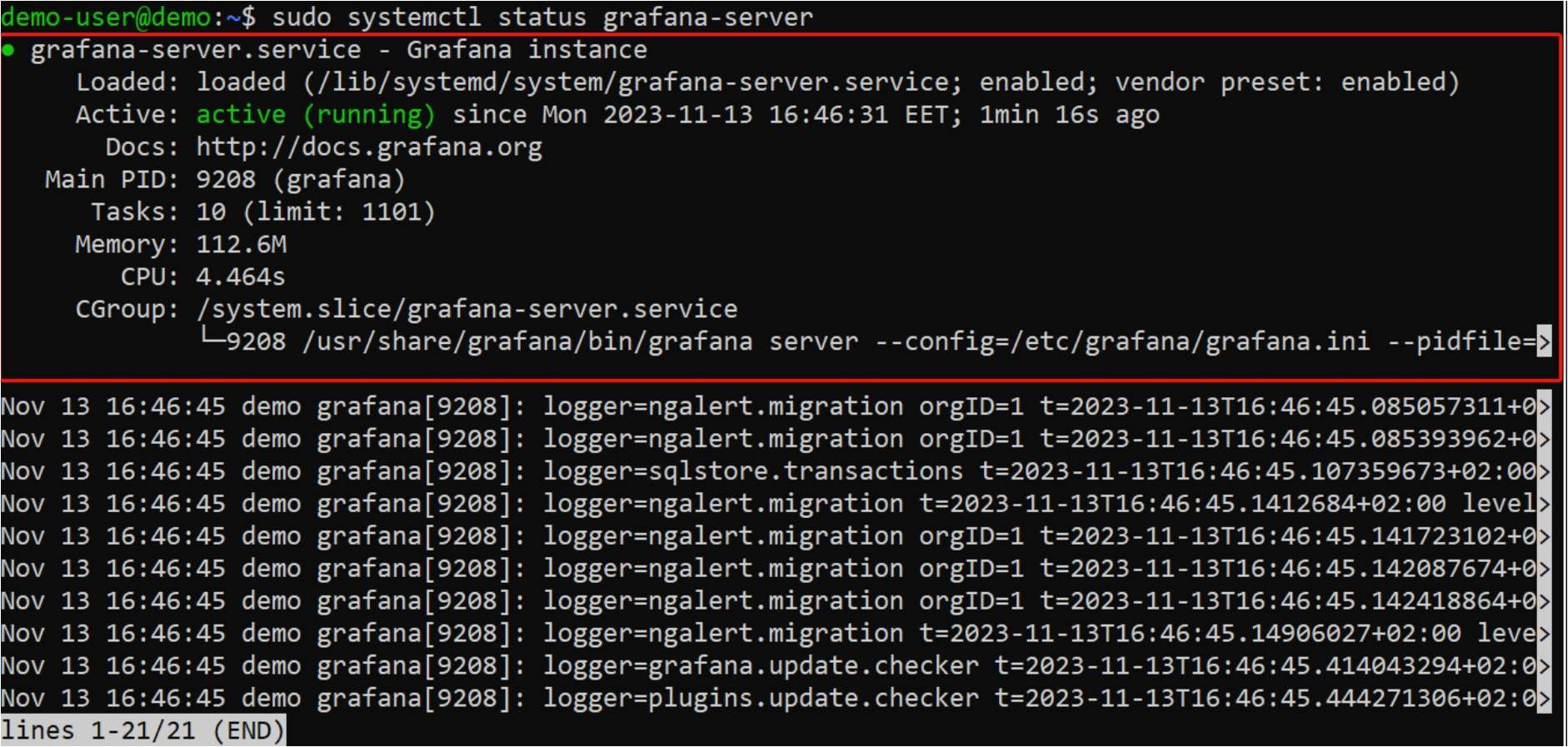
sudo systemctl start grafana-server sudo systemctl enable grafana- server



# **Step 6 - Verify that the Grafana service is running**

sudo systemctl status grafana-server

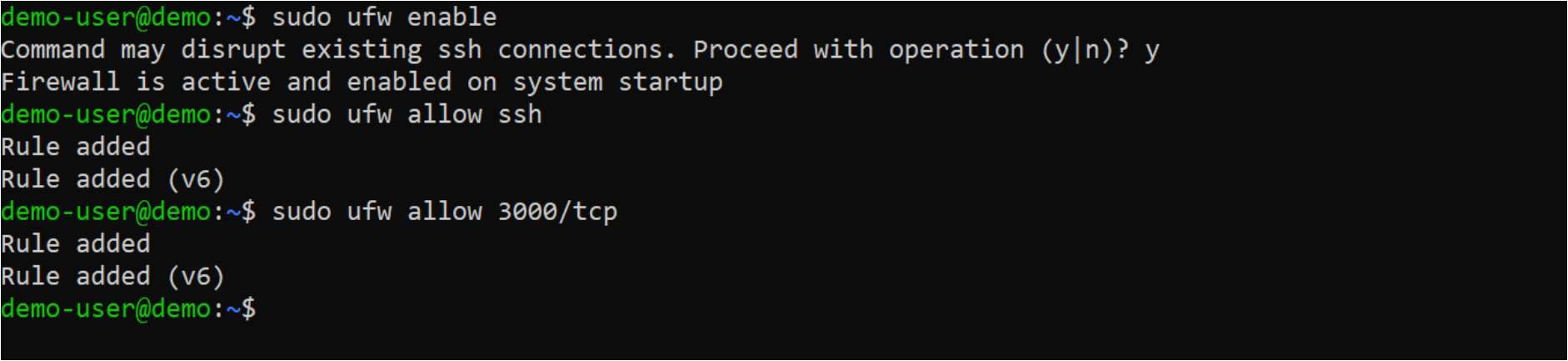
* If the Grafana service was started successfully, you should see a sign that it is active and running.



## **Step 7 - Open the port in the chrome**

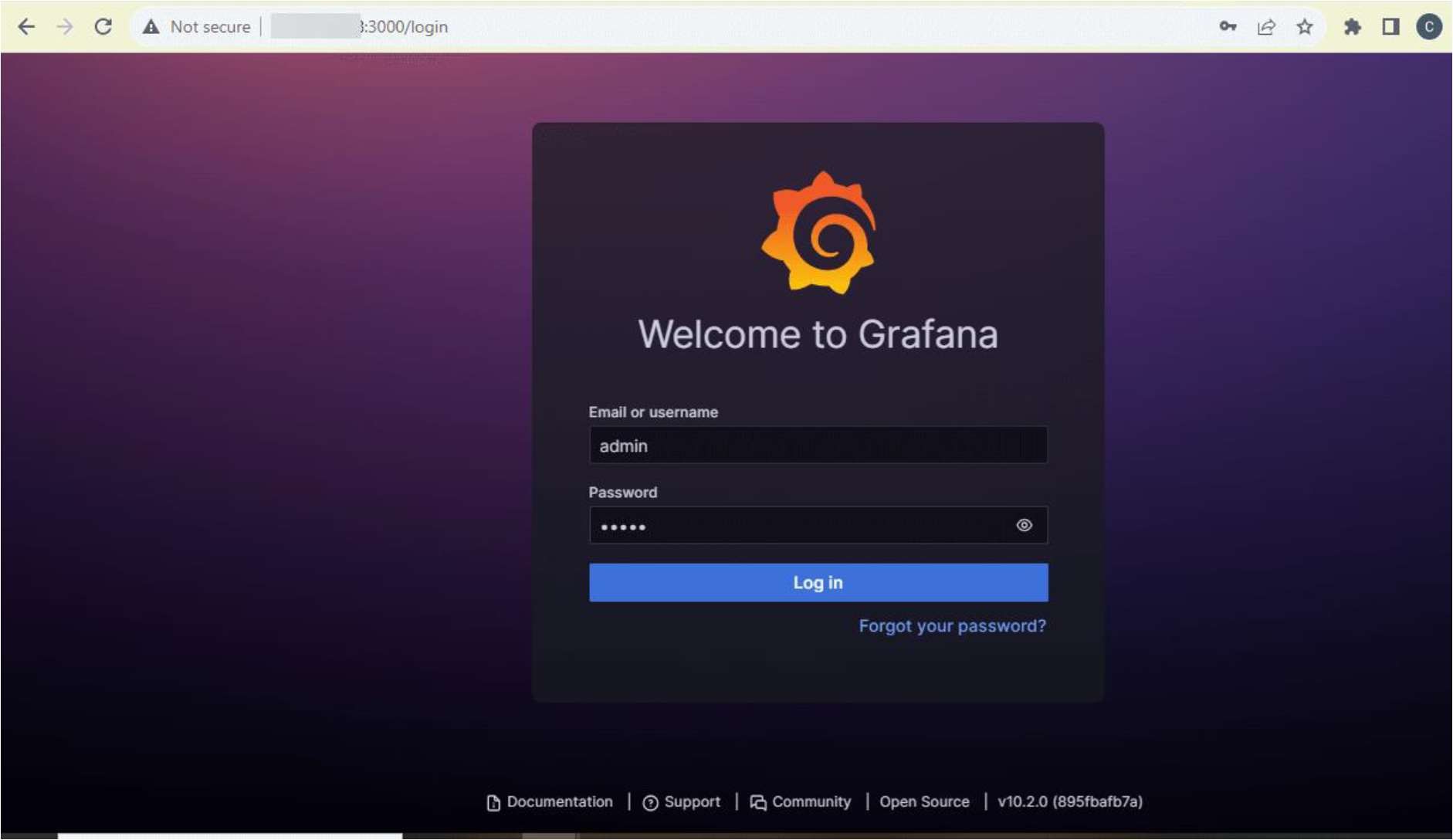
sudo ufw enable sudo ufw allow ssh

sudo ufw allow 3000/tcp



## **Testing & Access the Grafana web interface**

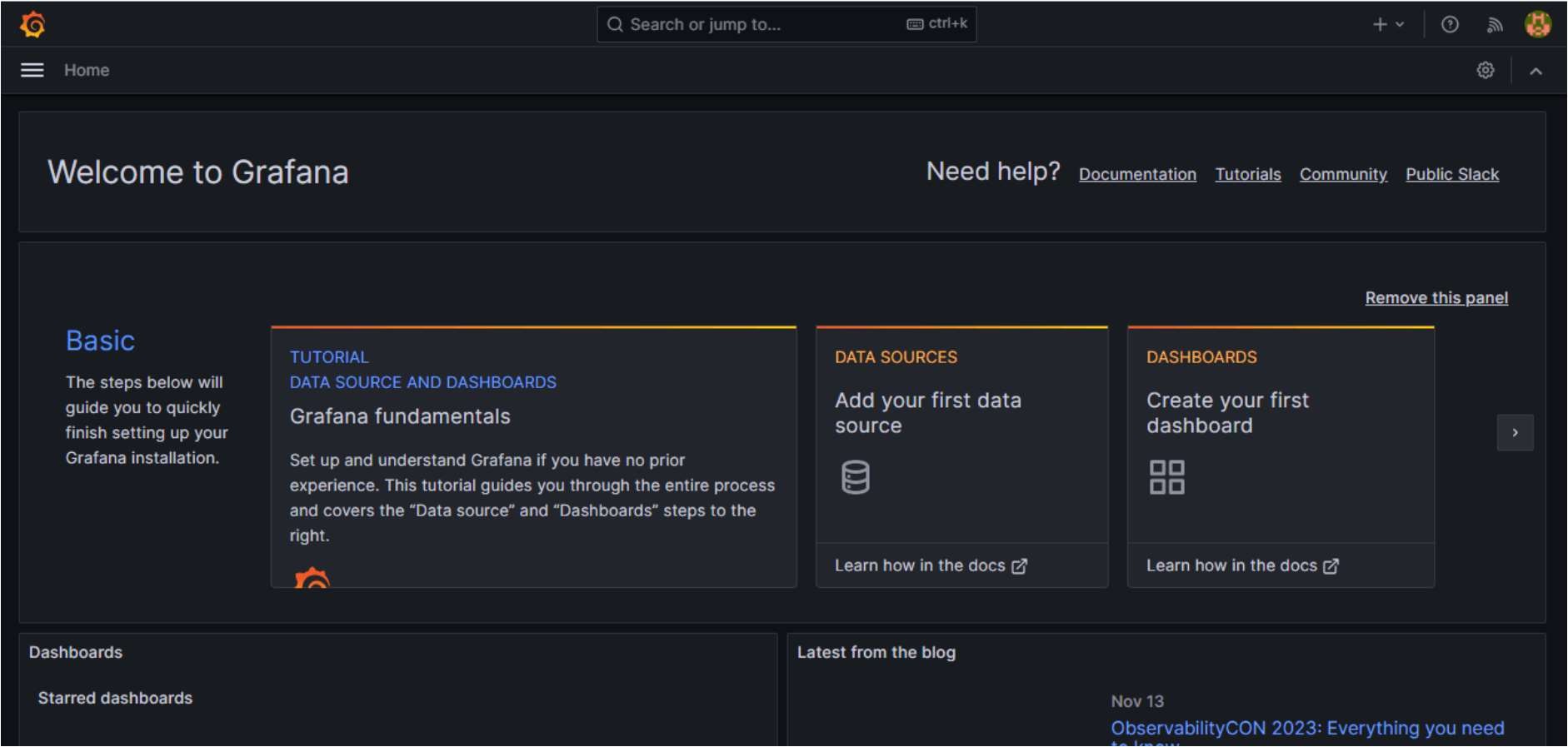
* To access the Grafana web interface, open a web browser and enter the IP address of your server (or hostname if applicable), followed by port 3000. The URL format should be http://your\_server\_IP:3000. Once loaded, you should see the Grafana login page. The default credentials are:
* **Username: admin**
* **Password: admin**



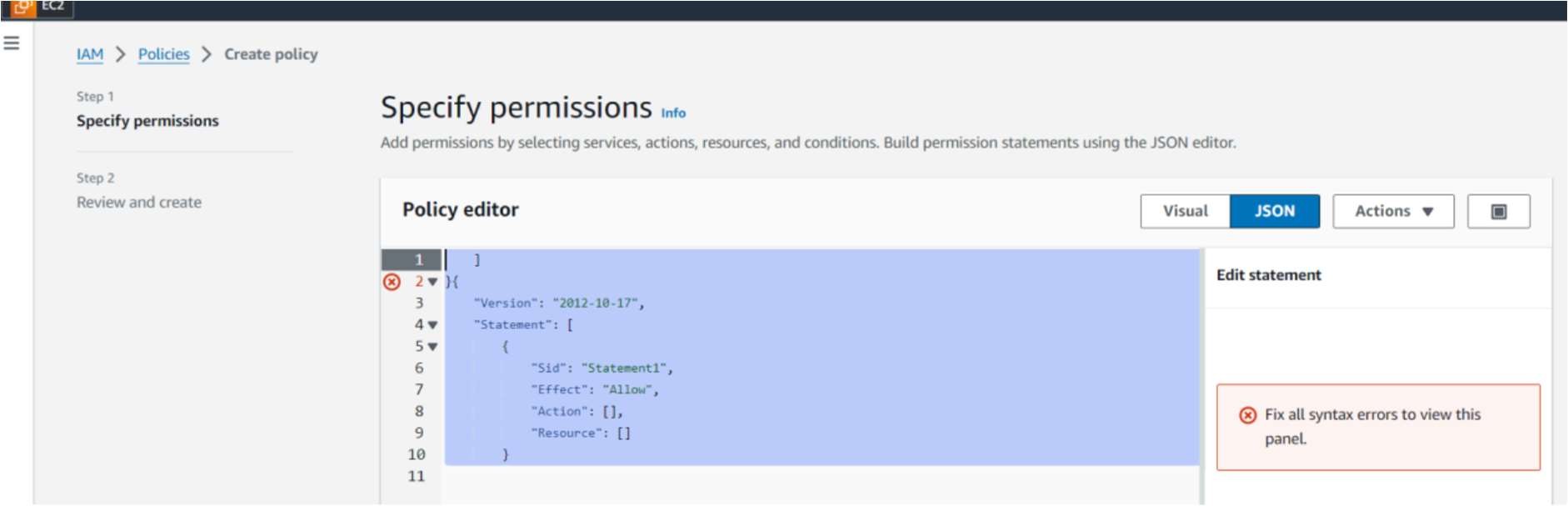
* You'll be prompted to create a new password. Input a secure password, confirm it, and click the "Submit" button.



* Once done, you'll have access to Grafana's dashboard.



* Now open the AWS console and select the option IAM. > Policies , Click on the **JSON** tab,
* Remove the existing code, and copy-paste the below policy



* **Statement into the editor:**

"Version": "2012-10-17",

"Statement": [

{

"Sid": "VisualEditor0", "Effect": "Allow", "Action": [ "ec2:DescribeInstances",

"cloudwatch:GetMetricData", "ec2:DescribeTags", "ec2:DescribeRegions", "cloudwatch:GetMetricStatistics", "cloudwatch:ListMetrics"

],

"Resource": "\*"

},

{

"Sid": "AllowReadingTagsInstancesRegionsFromEC2", "Effect":"Allow",

"Action": ["ec2:DescribeTags","ec2:DescribeInstances","ec2:DescribeRegions"], "Resource":"\*"

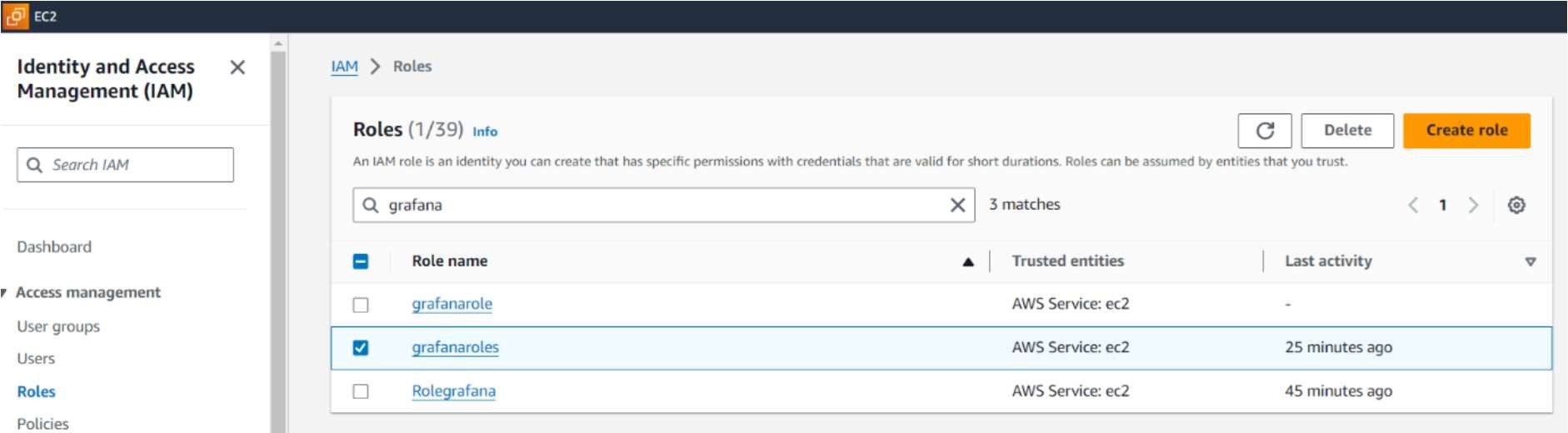
},

{

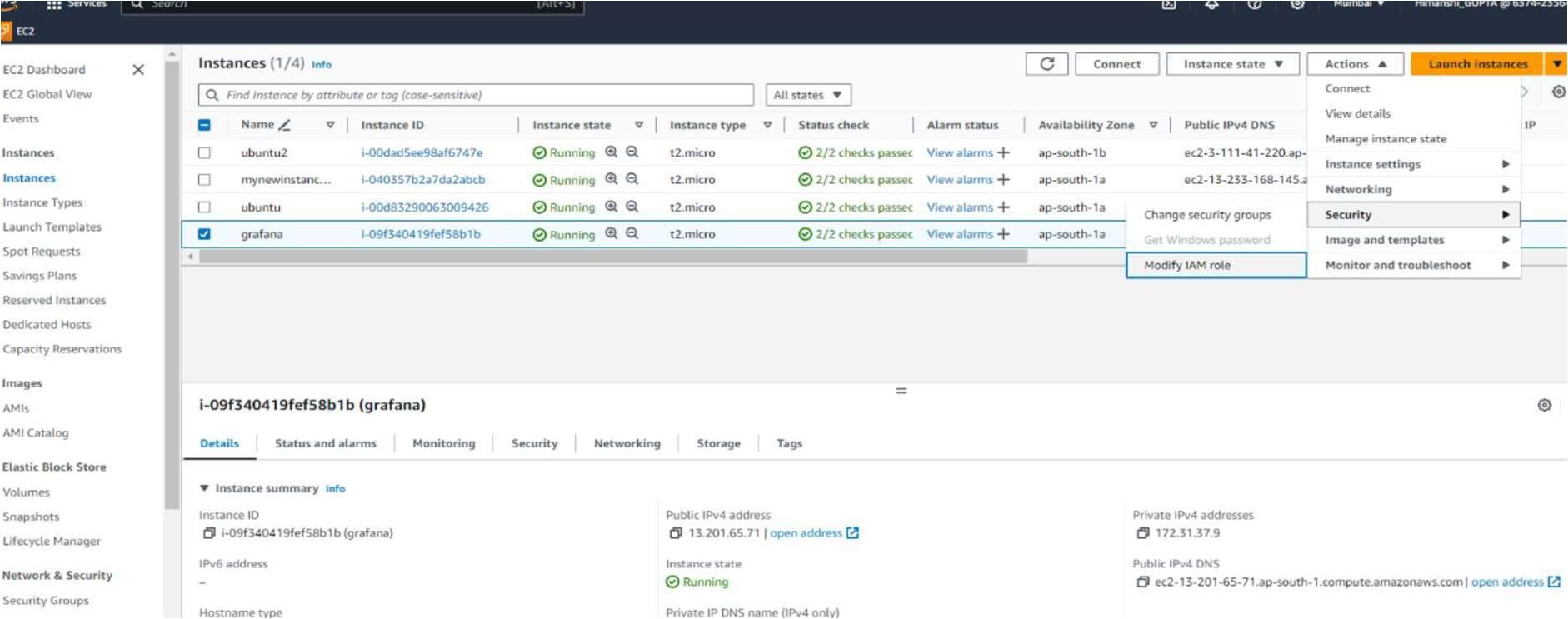
"Sid": "AllowReadingResoucesForTags", "Effect":"Allow", "Action":"tag:GetResources", "Resource":"\*"

}

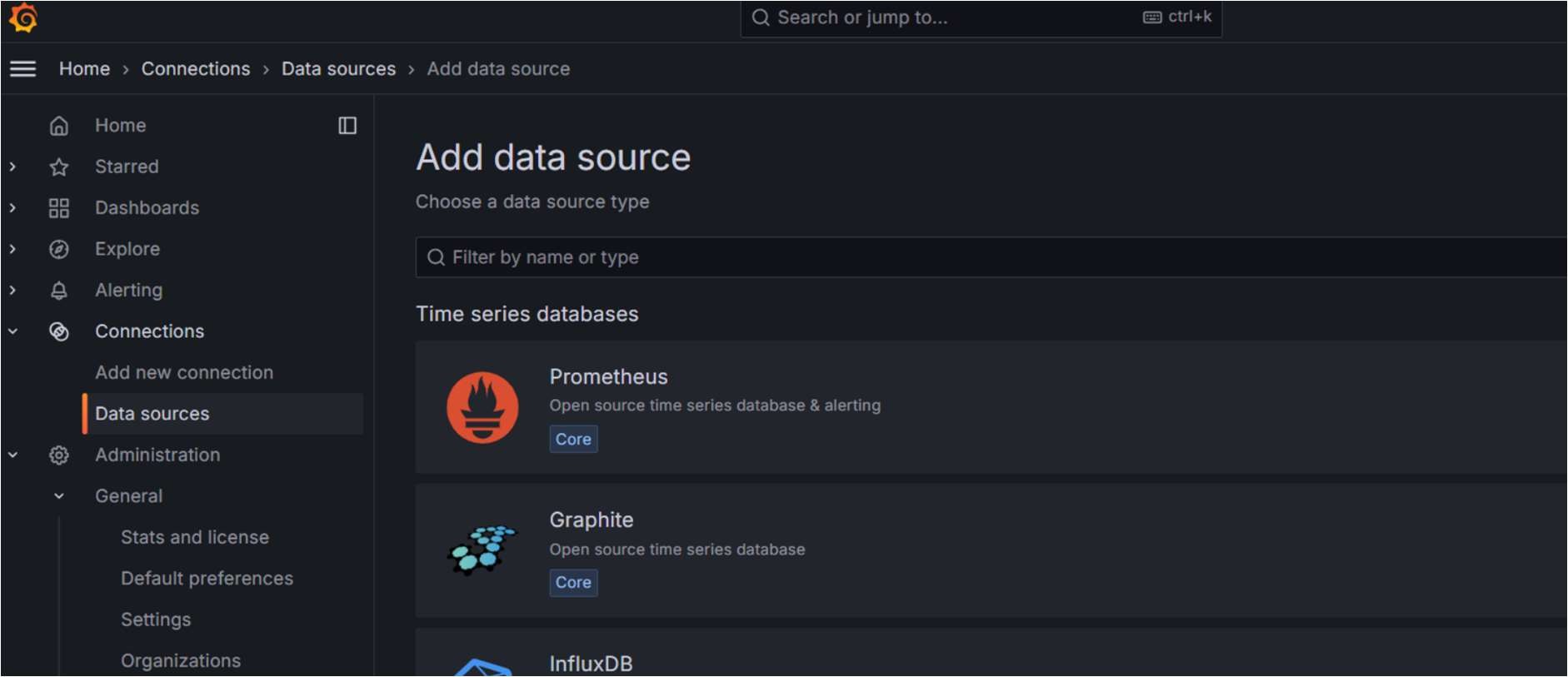
* Policy is created. Now click on the role tab. select the create role. Choose **Service or use case: EC2** click on the next. Select the policy and create a role. Your role is created-



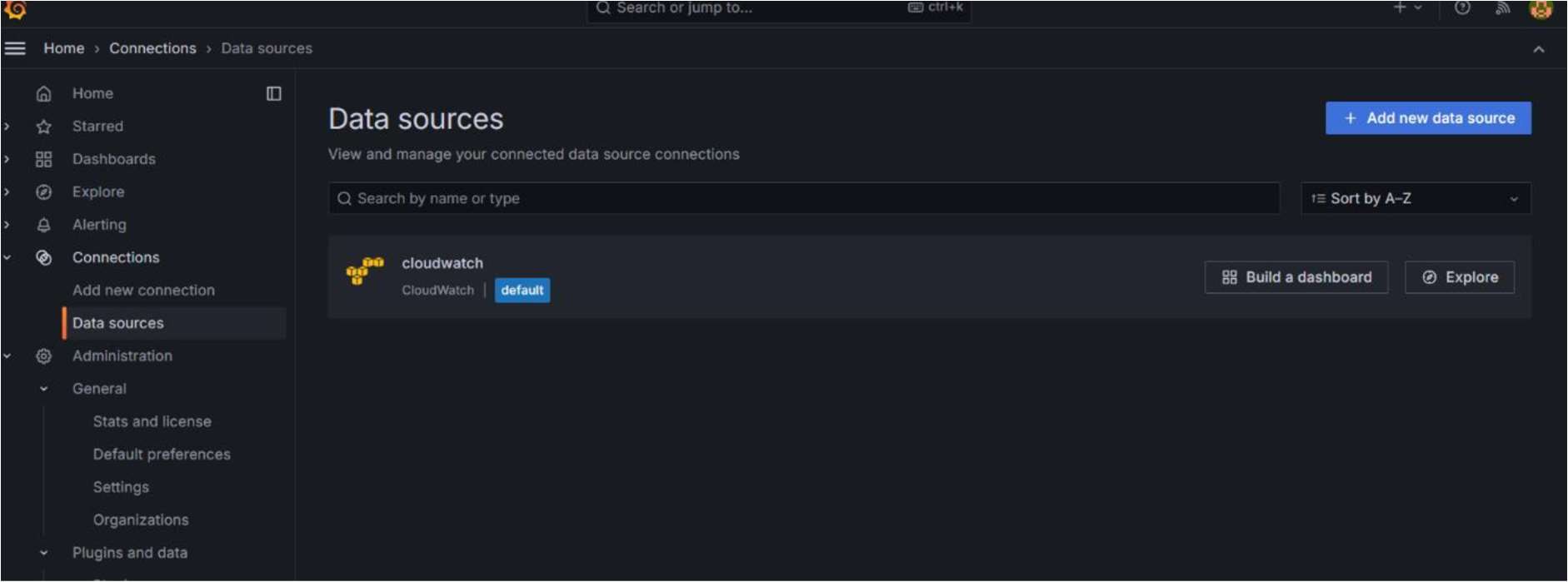
* Now go back to the Instances. Select your instance, click on the action tab, select the security, and then click on the Modify IAM role.



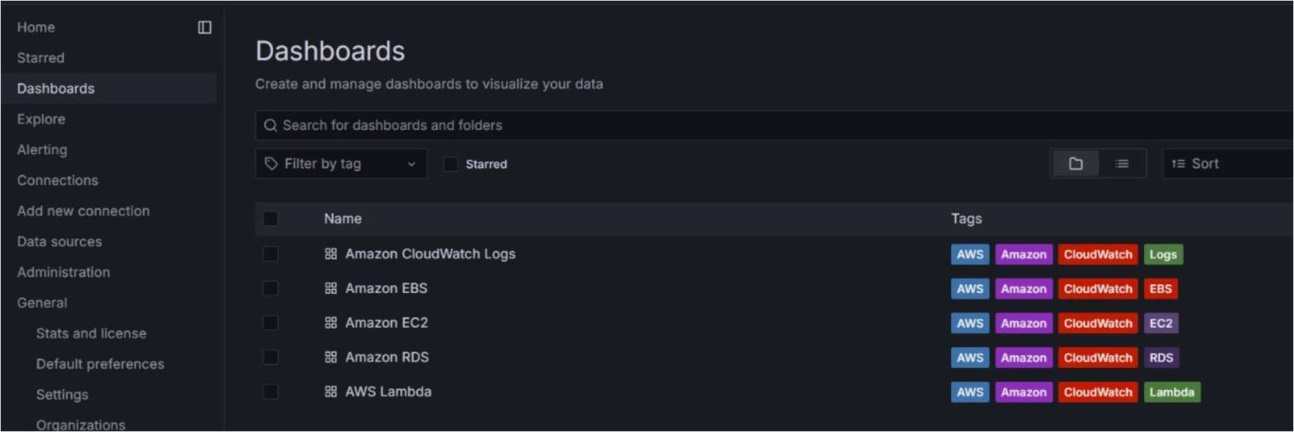
* Select your role then click on update IAM role. now it’s done to see your graph
* Go back to the Grafana dashboard. click on the connection tab and select the data source option.



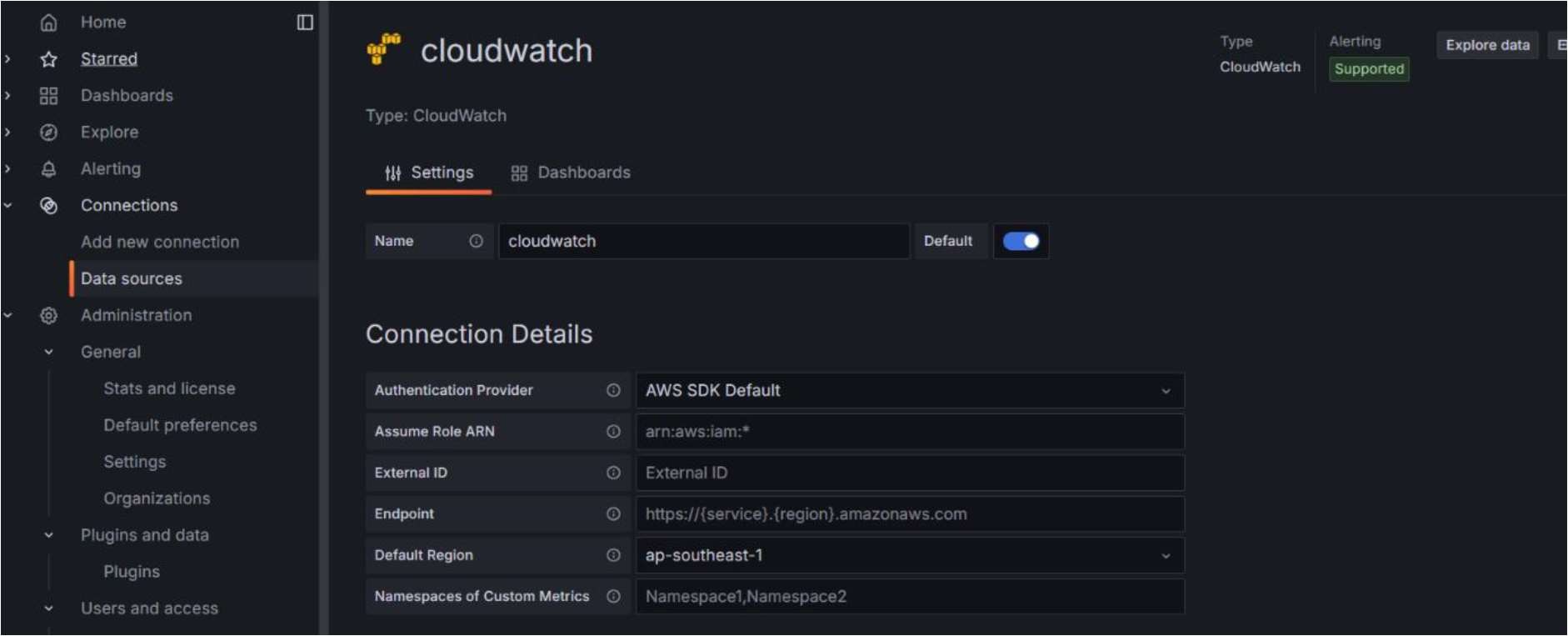
* Select the cloud watch



* Check it in the Dashboard. You see your screen like that-



* Click on the Amazon ec2 you see some errors.so click on the data source and change the region **ap-southe-1** like that -



* Save those changes.
* Go back to the Dashboard now you see your Grafana graph.

